DOI: https://doi.org/10.36059/978-966-397-295-4-37

АНТИКРИХКІСТЬ ТА АНТИКРИЗОВА СТІЙКІСТЬ В ДІДЖИТАЛ СЕРЕДОВИЩІ

Язвінська Надія Вікторівна
кандидат економічних наук,
доцент кафедри промислового маркетингу
Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»
Щербатюк Ірина Віталіївна
студенка
Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»

Антикризова стійкість в діджитал середовищі стає все більш актуальною темою для бізнесу, оскільки розвиток технологій дозволяє швидше та ефективніше реагувати на кризові ситуації. Але це також призводить до збільшення кількості загроз, з якими стикаються компанії в онлайн-середовищі.

Антикризова стійкість та антикрихкість – це два поняття, що відносяться до захисту діджитал-систем від впливу різних негативних чинників, але мають різне значення.

Антикризова стійкість означає здатність підприємства залишатися працездатною в умовах кризових ситуацій, таких як кібератаки, природні катастрофи, людські помилки тощо. Це означає, що підприємства може продовжувати працювати в обмеженому режимі або після перерви, доки не буде відновлена її повна функціональність. Антикризова стійкість зазвичай забезпечується захисними заходами, такими як резервне копіювання даних, захист від кібератак, мережеві протоколи забезпечення безпеки та інші [1, с. 75].

Антикрихкість – це здатність систематично створювати можливості розвитку, перетворюючи негативні наслідки помилок чи кризових ситуацій у нові можливості та ресурси. Це означає, що підприємство буде продовжувати працювати правильно незалежно від ситуації. Антикрихкість в діджитал середовищі зазвичай досягається за допомогою високоякісного програмного забезпечення, стандартизованих процесів розробки та тестування, а також ефективних методів налагодження системи [2, с. 111].

Отже, хоча обидва терміни стосуються захисту систем від негативного впливу, антикризова стійкість забезпечує захист від кризових ситуацій, тоді як антикрихкість забезпечує стійкість та надійність системи в будь-яких умовах.

Розглянемо аспекти антикризової стійкості діджитал систем на підприємстві:

– Захист від кібератак. Це охоплює впровадження захисних механізмів для запобігання атакам на системи компанії, а також постійне моніторинг та оновлення захисних технологій. Крім того, компанії повинні регулярно створювати резервні копії даних, щоб зменшити ризик втрати інформації під час технічних проблем.

– Використання хмарних технологій для збереження даних та резервного копіювання. Це дозволяє забезпечити доступність даних у будь-який час та звільнити компанію від необхідності зберігання власних серверів.

– Регулярно вдосконалення програмного забезпечення, щоб зменшити ризик технічних проблем та покращити безпеку даних.

– Навчання та підвищення кваліфікації персоналу є також важливим аспектом антикризової стійкості в діджитал середовищі.

– Розробка планів дій у випадку кризових ситуацій, таких як виток інформації, кібератаки, недоступність систем тощо. Компанії повинні бути готові до можливості будь-якої ситуації та мати готовість швидко та ефективно відповідати на них.

Однією з найбільш актуальних загроз є кібератаки, які можуть призвести до витоку конфіденційної інформації, втрати даних, недоступності систем та інших наслідків. У таких випадках компанії повинні діяти швидко та ефективно, щоб зменшити наслідки кризи та відновити роботу систем.

Ще одним важливим моментом антикризової стійкості є моніторинг онлайн-репутації компанії та швидка реакція на виявлені проблеми. Інтернет дозволяє користувачам швидко та легко ділитися своїми враженнями та відгуками про товари та послуги, тому важливо мати механізми для відстеження цих відгуків та швидко реагувати на негативні коментарі.

Враховуючи зростаючу роль діджитал середовища в сучасному бізнесі, антикризова стійкість в цьому контексті стає все важливішою для успішної діяльності компаній. На підприємствах повинні бути використані ефективні заходи захисту даних та інформації, розроблені плани дій у випадку кризових ситуацій та забезпечений достатній рівень кваліфікації персоналу. Такі заходи дозволяють зменшити ризики та забезпечити стійкість діджитал бізнесу у будь-яких умовах [3].

Антикрихкість є важливою характеристикою діджитал-систем, оскільки забезпечує їхню стійкість та надійність в будь-яких умовах. Деякі з аспектів антикрихкості в діджитал середовищі включають наступне:

– Відповідність стандартам та нормам: Для забезпечення анти-крихкості діджитал-систем потрібно дотримуватися стандартів та норм,

які забезпечують високу якість програмного забезпечення та процесів розробки.

– Надійність системи: Діджитал-системи повинні бути надійними та стійкими до впливу помилок, відмов та відмінностей в роботі, що можуть виникнути через різні причини.

– Резервне копіювання даних: Резервне копіювання даних дозволяє зберігати дані у випадку відмови системи або катастрофи. Це дозволяє забезпечити доступ до важливих даних та запобігти їх втраті.

– Ефективна стратегія управління помилками: Ефективна стратегія управління помилками дозволяє виявляти та виправляти помилки у системі до того, як вони призведуть до серйозних проблем.

– Забезпечення безпеки: Діджитал-системи повинні бути захищені від кібератак та інших загроз безпеці. Для цього можуть використовуватись різноманітні методи, такі як шифрування даних, фізичний захист, мережеві протокол [3].

Отже, хоч антикрихкість та антикризова стійкість пов’язані зі забезпеченням стійкості діджитал систем, вони мають різний підхід та фокусуються на різних аспектах забезпечення безпеки та стабільності.

Список використаних джерел:

1. Токмакова І. В, Панченко Н. Г., Кургузова М. Ю. Розроблення антикризової стійкості в умовах цифрової трансформації. *Економіка підприємства.* С. 70–79.

2. Язвінська Н. В., Вишницька С. В. Формування антикрикої конкурентоздатності підприємства – маркетинговий підхід. *Економічний вісник НТУУ «Київський політехнічний інститут»*. Київ. 2022. С. 107–113.

3. Thrive during a crisis: the role of digital technologies in fostering antifragility in small and medium-sized enterprises. *Journal of Ambient Intelligence and Humanized Computing*. URL: https://d-nb.info/1259788016/34.